УДК 621.391:519.7

С. М. КОНЮШОК, кандидат технічних наук
А М. ОЛЕКСІЙЧУК, доктор технічних наук

БЕЗУМОВНО СТІЙКІ СХЕМИ РОЗПОДІЛУ КЛЮЧІВ В ІНФОРМАЦІЙНИХ ТА ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ З ВЕЛИКОЮ КІЛЬКІСТЮ АБОНЕНТІВ: І. СХЕМИ ПОПЕРЕДНЬОГО РОЗПОДІЛУ Й УЗГОДЖЕННЯ КЛЮЧІВ

Вступ

Проблеми створення криптографічно стійких та ефективних протоколів розподілу ключів криптосистем, що використовуються для захисту інформації в спеціальних телекомунікаційних системах (СТКС), займають центральне місце в сучасній криптографії. Незважаючи на відчутний прогрес, що досягнутий в цьому напрямі за останнє десятиріччя, більшість актуальних наукових задач залишаються невирішеними, стимулюючи продовження активних досліджень у різних галузях науки й техніки, що пов'язані з розробкою, застосуванням та аналізом криптографічних протоколів розподілу ключів.

Стримкий розвиток засобів зв'язку та телекомунікацій, ускладнення топології інформаційних і обчислювальних мереж, поява нових інформаційних технологій, поряд з розширенням сфери застосування та підвищенням можливостей засобів криптографічного захисту інформації, призводять до перегляду традиційних концепцій і методології вирішення задач захисту інформації в СТКС, розробки нових наукових та технологічних рішень як у самої криптографії, так і в її застосуваннях.

Одним з таких перспективних застосувань, що активно розвиваються протягом останнього часу, є системи захищеного багатоадресного зв'язку, абоненти яких здійснюють сумісне виконання певних завдань шляхом інтерактивної взаємодії. Даними завданнями можуть бути звичайний обмін інформацією між змінною за своїм складом групою користувачив, сеанс конференс-зв'язку (наприклад, інтерактивне обговорення порядку денного майбутнього засідання), відеоконференція з участю формальних представників різних країн або сумісне виконання групою користувачив розподіленої обчислювальної мережі алгоритму розв'язання деякої складної задачі [1 – 6]. За виконанням будь-якого з перерахованих завдань для забезпечення надійного криптографічного захисту інформації, що циркулює в системі багатоадресного зв'язку, необхідно враховувати специфічні особливості даної системи, які пов'язані з наявністю в ній великої кількості авторизованих користувачів, що утворюють наділені різними правами групи, склад яких може динамічно змінюватись протягом часу [7, 8].

Серед різноманітних криптографічних протоколів, які використовуються для розподілу секретних ключів, наибільш перпективними для застосування в системах захищеного багатоадресного зв'язку вважаються безумовно стійкі схеми розподілу ключів (БССРК) [1, 9 – 12].

Неформально схема розподілу ключів (СРК) являє собою метод, з використанням якого довірена сторона, що виконує функції центру розподілу ключів (ЦРК), здійснює передачу деякої допоміжної інформації абонентам

спеціальної телекомунікаційної системи таким чином, що згодом абоненти, які належать кожній заздалегідь визначеній групі, здатні відновити за цією (та, можливо, певною іншою) інформацією спільний секретний ключ. Схема розподілу ключів, криптографічна стійкість якої не залежить від обчислювальних можливостей противника, називається безумовно стійкою [1, 10, 13].

На сьогодні задачі розробки методів синтезу, аналізу математичних моделей та дослідження властивостей різноманітних класів безумовно стійких схем розподілу ключів складають один із перспективних напрямів сучасної криптографії та включають у себе широке коло окремих задач, які характеризуються різною прикладною спрямованістю. Спектр можливих застосувань БССРК є надзвичайно широким, починаючи від систем платного телемовлення, захисту від несанкціонованого копіювання та безпечного розподілу відкритими мережами зв'язку аудіо- й відеопродукції, і закінчуючи криптографічним захистом інформації в системах багатоадресного зв'язку та розподілених сенсорних мережах (див. нижче пункти 1 – 3). Свідченням про зростаючий інтерес до цього напряму з боку зарубіжних фахівців-криптографів є велика кількість публікацій та доповідей на міжнародних наукових конференціях, що присвячені як теоретичним аспектам безумовно стійких схем розподілу ключів, так і їх численним застосуванням (див. перелік джерел, що приведено нижче). Нажаль, слід констатувати, що для вітчизняної криптографічної науки згаданий напрям залишається на сьогодні terra incognita, про що свідчить практично повна відсутність наукових публікацій за даною тематикою українською або російською мовами.

Автори даної статті здійснили спробу надати перше систематичне викладення українською основ та нещодавніх досягнень теорії БССРК. (Відмітимо, що остання велика оглядова праця за цією темою, написана англійською [10], опублікована в 1997 році).

Стаття складається з двох частин. У першій частині приведена загальна класифікація існуючих протоколів розподілу ключів та викладені результати аналізу сучасного стану, проблематики і напрямів досліджень у галузі побудови безумовно стійких схем попереднього розподілу й узгодження ключів в інформаційних та телекомунікаційних системах з великою кількістю абонентів. Друга частина статті присвячена детальному викладенню перспективних методів синтезу безумовно стійких схем багатоадресного розподілу ключів (СБРК).

Слід відзначити, що при роботі над оглядом головна увага приділялась конструктивним методам побудови та аналізу ефективності безумовно стійких схем розподілу ключів, які основуються на різних комбінаторних конфігураціях. Зокрема, за межами викладення залишились методи синтезу БССРК на основі орієнтованих графів [8], стислий огляд яких подано в нещодавній роботі [14], та аналітичні нижні границі інформаційних показників ефективності БССРК (див. [1]). Лише мимохідь згадані обчислювально стійкі схеми розподілу ключів (ОССРК) [14, 15], аналіз відомих методів побудови яких заслуговує окремого огляду.

Автори сподіваються, що з'явлення цієї роботи допоможе вітчизняним фахівцям глибше ознайомитись із безумовно стійкими схемами розподілу

ключів, які складають важливий та перспективний об’єкт досліджень у сучасній криптографії.

1. Класифікація та аналіз перспективних протоколів розподілу ключів в інформаційних та телекомунікаційних системах з великою кількістю абонентів

Згідно [16 – 18], розрізняють наступні *типи криптографічних протоколів розподілу ключів* (рис. 1): *протоколи передачі ключів, що згенеровані заздалегідь*; *протоколи сумісного вироблення спільного ключу* (*відкритого розподілу ключів*); *схеми розподілу ключів*.

До протоколів першого типу відносяться такі алгоритми передачі ключів, що виконуються багатьма діючими сторонами, за якими зазначені сторони заздалегідь володіють будь-якою відомою їм секретною інформацією [16]. Існують *двосторонні протоколи*, згідно яким сторони здійснюють передачу ключів за безпосередньою взаємодією, та *протоколи централізованого розподілу* (*згенерованих*) *ключів*, які передбачають наявність третьої сторони, що відіграє роль довіреного центру. При цьому для передачі ключів у таких протоколах можуть застосовуватись як симетричні, так і асиметричні криптосистеми [16, 18, 19].

Певним недоліком зазначених протоколів є принципова неможливість їхнього використання для організації сеансів одночасного захищеного зв’язку між більш ніж двома сторонами (так званих сеансів конференс-зв’язку) [16]. На практиці з метою уникнення цього недоліку та збільшення терміну дії секретних ключів, які зберігають кореспонденти СТКС, передбачається застосовувати їхні секретні ключі виключно для зашифрування-розшифрування сеансових ключів, що передаються їм з центру розподілу ключів та використовуються для шифрування інформації на протязі сеансу конференс-зв’язку. Такі протоколи вимагають від кожного абонента зберігати лише один власний секретний ключ для зв’язку з ЦРК і дозволяють організовувати сеанси конференс-зв’язку без обмеження кількості учасників. Якщо число абонентів, які бажають прийняти участь у сеансі конференс-зв’язку, дорівнює N, то для передачі секретного сеансового ключу кожному абоненту ЦРК повинен послідовно передати N шифрованих повідомлень.

Таким чином, в цілому, існуючі протоколи передачі згенерованих ключів [16, 18, 19] вимагають або збереження кожним абонентом великої кількості ключів, або часу затримки сеансу зв’язку, що призначений для отримання абонентами сеансових ключів від ЦРК. До того ж, ініціалізація таких протоколів передбачає доставку кожному абоненту СТКС його власних ключів захищеним каналом зв’язку.

На відміну від розглянутих вище, протоколи відкритого розподілу ключів дозволяють виробляти взаємодіючим сторонам спільні секретні ключі шляхом динамічної взаємодії на основі обміну відкритими повідомленнями без застосування будь-якої таємної інформації, що розподілена заздалегідь [16]. Важливою особливістю відкритого розподілу ключів є те, що жодна із взаємодіючих сторін не має можливості визначити заздалегідь значення секретного ключу, оскільки ключ залежить від повідомлень, що передаються в процесі обміну відкритою інформацією.

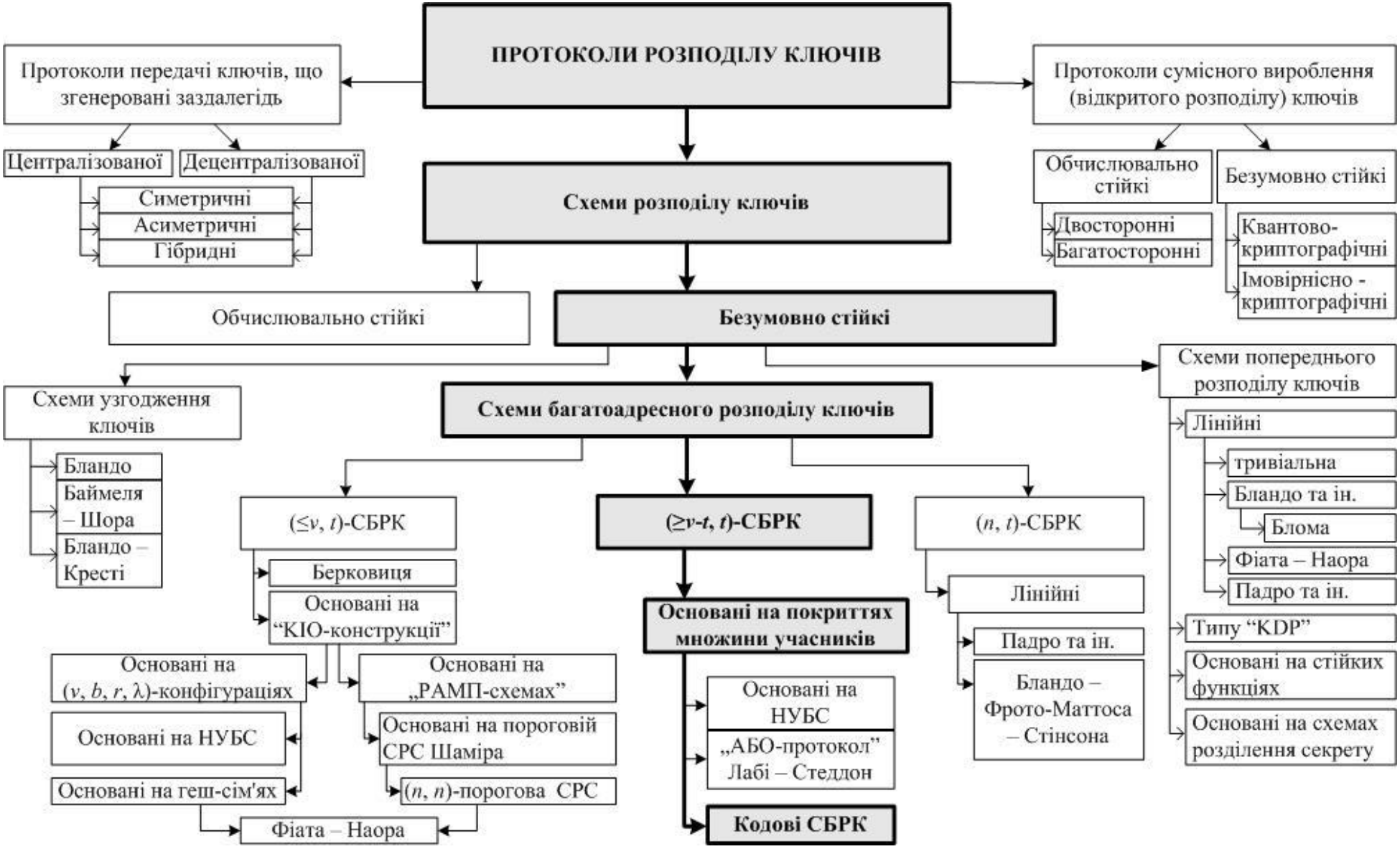

Рис. 1. Класифікація протоколів розподілу ключів

На сьогоднішній день можна виділити два потужних класи криптографічних протоколів відкритого розподілу ключів (див. рис. 1): *обчислювально стійкі протоколи*, які ґрунтуються на принципах асиметричного шифрування [16, 18 – 20]; *безумовно стійкі протоколи*, що основуються на певних припущеннях відносно фізичних властивостей каналів зв'язку, якими здійснюється передача повідомлень, або припущеннях щодо умов інформаційної взаємодії, можливостей супротивника та інших [21 – 26].

Оскільки стійкість переважної більшості сучасних асиметричних криптосистем базується на (недоведеному) припущенні про обчислювальну складність алгоритмів вирішення певних математичних задач, то протоколи відкритого розподілу ключів з використанням асиметричних криптографічних перетворень також мають лише обчислювальну (та, строго кажучи, не обґрунтовану) стійкість. При цьому вдосконалення математичних методів розв'язання зазначених задач і розвиток обчислювальної техніки примушують до постійного збільшення довжини ключових даних у сучасних асиметричних криптосистемах, що, в свою чергу, збільшує час затримки при організації сеансів зв'язку. Відомо також [1, 11, 27], що зашифрування та розшифрування повідомлень з використанням діючих асиметричних криптосистем відбувається на декілька порядків повільніше, ніж у діючих симетричних (як блокових, так і потокових) криптосистемах. Для забезпечення необхідної стійкості шифрування асиметричні криптоалгоритми вимагають застосування ключів, довжина яких значно (у 2 та більше разів) перевищує довжину ключів діючих симетричних криптосистем [19, 28].

Отже, застосування в асиметричних протоколах відкритого розподілу ключів будь-якої довіреної сторони, що виконує функції генерування та розподілу сеансових ключів абонентам СТКС, приводить до великої часової затримки між запитом на сеанс зв'язку та моментом отримання необхідного ключа кожним абонентом. Зрозуміло, що зростання числа абонентів неодмінно збільшує і час такої затримки. Спроба відмовитись від послуг довіреної сторони і формувати спільний сеансовий ключ шляхом обміну відкритими повідомленнями між групою абонентів також викликає часові затримки, що пов'язані з великим обсягом повідомлень, якими мають обмінятися ці абоненти.

В якості приклада протоколу, за допомогою якого група з N абонентів може сформувати спільний ключ в результаті обміну відкритими повідомленнями, приведемо модифікацію відомого протоколу Діффі–Хеллмана [19]. Цей протокол вимагає від кожного абонента передачі $N-1$ повідомлень. Отже, потрібно обмінятись $N(N-1)$ відкритими повідомленнями з метою отримання кожним абонентом спільного секретного сеансового ключу.

Другий клас протоколів відкритого розподілу ключів складають безумовно стійкі криптографічні протоколи, в основу яких покладені принципи квантової [25, 26, 29 – 32] та, відповідно, імовірнісної криптографії [21, 22, 33 – 35]. До останніх відносяться, зокрема, безумовно стійкі протоколи узгодження ключів у моделях систем передачі інформації з відвідним каналом (wire-tap channel) [23, 36 – 43] та обмеженою пам'яттю (bounded storage model) [24, 44 – 46]. Проте, зазначені перспективні напрями в галузі побудови криптографічних

протоколів розподілу ключів на даний час знаходяться ще на етапі інтенсивних теоретичних досліджень. Практичне застосування таких протоколів в інформаційних та телекомунікаційних системах з великою кількістю абонентів вимагає, перш за все, вирішення складних теоретичних та інженерних задач, що мають принциповий характер [21].

Таким чином, застосування практичних (“асиметричних”) протоколів відкритого розподілу ключів, з одного боку, дозволяє позбавитись від використання захищених каналів зв’язку для передачі секретних сеансових ключів абонентам СТКС, а з іншого боку – забезпечує лише обчислювальну стійкість процедури вироблення спільного ключу абонентів при значному зростанні часу, що необхідний для організації кожного сеансу захищеного зв’язку.

Третій тип криптографічних протоколів (див. рис. 1) складають схеми розподілу ключів, за якими довірений центр здійснює передачу деякої допоміжної секретної інформації абонентам телекомунікаційної системи (мережі зв’язку) таким чином, що тільки визначені, *привілейовані*, групи абонентів здатні виробити на основі цієї (та, можливо, іншої, відкритої) інформації спільний *груповий ключ*. При цьому передбачається, що жодна з так званих *заборонених* коаліцій (або груп) абонентів, які не мають право на володіння ключами привілейованих груп, не може відновити такі ключі [1, 9, 10, 14, 47].

Схеми розподілу ключів поділяються на безумовно стійкі та обчислювально (або умовно) стійкі СРК. За визначенням схема розподілу ключів називається *безумовно стійкою*, якщо учасники жодної забороненої коаліції не мають принципової можливості отримати будь-яку інформацію про ключі відповідних привілейованих груп, навіть за умовою, що вони володіють необмеженими обчислювальними або ємнісними ресурсами [10]. У протилежному випадку СРК має назву *обчислювально стійкої* схеми розподілу ключів [9].

За визначенням СРК складається з двох алгоритмів (або етапів): алгоритму розподілу вихідної секретної ключової інформації; алгоритму формування групових ключів, що відповідають привілейованим групам абонентів [1, 10, 14]. Останній алгоритм виконується окремо кожним абонентом відповідної привілейованої групи із застосуванням власної секретної інформації, що він отримує з ЦРК на першому етапі, та (можливо) відкритої інформації, яку він отримує мережею зв’язку. Відкрита інформація може зберігатись на мережевому сервері, бути отриманою від інших абонентів даної групи або бути переданою з ЦРК.

Стійкість відомих на сьогоднішній день ОССРК [9, 14, 15, 48 – 53], як і, взагалі, умовно стійких криптографічних систем, ґрунтується на недоведених припущеннях щодо складності відомих математичних задач (дискретного логарифмування, факторизації цілих чисел та інших [16, 18, 19]) або існування важкооборотних функцій чи генераторів псевдовипадкових послідовностей [54]. Отже, зазначені вище вади, з точки зору криптографічної стійкості, що притаманні обчислювально стійким протоколам відкритого розподілу ключів, характерні й для умовно стійких СРК.

Далі головна увага зосереджена на аналізі відомих методів побудови та властивостей безумовно стійких схем розподілу ключів. *Нижче термін* "*схема розподілу ключів*" *позначає виключно деяку безумовно стійку СРК, якщо не застережене супротивне.*

Загальновизнаним є поділ безумовно стійких СРК на три великих класи (див. рис. 1): *схеми попереднього розподілу ключів* (СПРК), *схеми узгодження ключів* (СУК) та *схеми багатоадресного розподілу ключів* або *схеми* "*широкомовного шифрування*" (broadcast encryption schemes) [1, 10, 13].

Основною ознакою, за якою проводиться зазначена класифікація БССРК, є саме другий етап (алгоритм) схеми. Так, у схемах попереднього розподілу ключів обчислення групового ключу на другому етапі здійснюється окремо кожним абонентом даної привілейованої групи тільки на основі власної секретної інформації, що він отримує з ЦРК, та загальнодоступної, незмінної відкритої інформації (наприклад, ідентифікаторів решти абонентів даної привілейованої групи). У схемах узгодження ключів вироблення групового ключу відбувається в результаті взаємодії абонентів привілейованої групи, згідно з визначеним протоколом. В схемах багатоадресного розподілу ключів на другому етапі з центру розподілу ключів здійснюється широкомовна передача певного повідомлення всім (не тільки привілейованим) абонентам мережі зв'язку. Далі на основі цього повідомлення та секретної інформації, що отримана на першому етапі, абоненти відповідної привілейованої групи можуть обчислити секретний груповий ключ. Слід підкреслити, що при цьому властивості СБРК гарантують принципову неможливість отримання жодною із заборонених коаліцій абонентів будь-якої інформації про груповий ключ даної привілейованої групи.

Сучасні схеми розподілу ключів і, зокрема, схеми "широковомовного шифрування" складають один з найбільш перспективних класів криптографічних протоколів розподілу ключів в інформаційних та телекомунікаційних системах із великою кількістю або високодинамічним складом учасників. На цей час (як обчислювально стійкі, так і безумовно стійкі) СРК мають достатньо велику кількість практичних застосувань, які поділяються на декілька основних напрямів [1, 15]. Це – системи захищеного багатоадресного зв'язку [2 – 6], у яких привілейовані групи абонентів динамічно змінюються шляхом підключення або відключення від мережі зв'язку; системи "вистежування порушника" [55 – 66], що призначені до пошуку так званих нечесних користувачів, які застосовують нелегальні пристрої дешифрування інформації; схеми скасування прав доступу [15, 52, 53, 67 – 69], які дозволяють ефективно та швидко відміняти права доступу до інформації певним невеликим групам користувачів. Крім того, ряд існуючих схем багатоадресного розподілу ключів надає можливість ефективно вирішувати задачі, які знаходяться на перехресті декількох з перерахованих вище напрямів. Це, наприклад, здатність багатоадресної передачі та "вистежування порушника" [14, 70 – 72], можливість одночасно вистежувати та відміняти права доступу [15, 52, 53] та інші.

Отже, серед найбільш важливих переваг БССРК у порівнянні з іншими протоколами розподілу ключів (див. рис. 1) слід відзначити [1, 9, 10, 13]

1) безумовну стійкість БССРК, що не основується на припущеннях відносно фізичних властивостей каналів зв'язку або умов, за якими відбувається процес інформаційної взаємодії;

2) можливість теоретичного обґрунтування (за адекватними, з практичної точки зору, припущеннями) стійкості криптографічних протоколів розподілу ключів, що основуються на БССРК;

3) можливість забезпечення потрібної криптоживучості телекомунікаційних систем або мереж зв'язку з великою кількістю абонентів за умовою достатньої практичності систем розподілу ключів, що побудовані на основі БССРК;

4) спроможність зменшення кількості секретної ключової інформації, що зберігають абоненти СТКС, без втрати потрібної криптоживучості (стійкості до компрометацій абонентів);

5) можливість інтерактивного розподілу групових ключів абонентам СТКС без використання (за виключенням етапу інсталяції БССРК) індивідуальних захищених каналів зв'язку з ними;

6) можливість швидкого відключення заборонених (скомпрометованих) та підключення нових привілейованих абонентів із порівняно невеликою складністю цих операцій.

Перераховані властивості дозволяють виділити з існуючих протоколів розподілу ключів клас БССРК як найбільш перспективний для застосування в інформаційних та телекомунікаційних системах з великою кількістю абонентів.

Більш детальний аналіз властивостей БССРК передбачає, перш за все, надання формальних, математичних визначень та уточнення показників ефективності зазначених схем розподілу ключів. Викладенню цих понять присвячений наступні пункти статті.

2. Математичні моделі та показники ефективності безумовно стійких схем розподілу ключів

Як відмічено вище, кожна БССРК складається з двох етапів: попереднього розподілу з ЦРК допоміжної секретної інформації абонентам спеціальної телекомунікаційної системи (мережі зв'язку) та, відповідно, обчислення абонентами, що належать довільній привілейованій групі, спільного групового ключу.

Позначимо $V = \{1, 2, \ldots, v\}$ множину абонентів спеціальної телекомунікаційної системи, 2^V – сукупність всіх підмножин множини V. У найбільш загальному випадку перелік привілейованих та заборонених груп учасників БССРК визначається за допомогою так званої *структури специфікації* схеми розподілу ключів, що представляє собою довільну підмножину $\Gamma \subseteq V^2$ таку, що для будь-якої пари множин $(P, C) \in \Gamma$ виконується умова $P \cap C = \varnothing$ [13]. Множина $P \subseteq V$ називається *привілейованою* (або Г-*привілейованою*) *групою* учасників, якщо існує множина $C \subseteq V$ з властивістю $(P, C) \in \Gamma$. Позначимо символом $\Re$ сукупність всіх привілейованих груп учасників даної БССРК. Для кожного $P \in \Re$ позначимо $\Im_P$ сукупність всіх множин $C \subseteq V$ таких, що $(P, C) \in \Gamma$. Зазначені множини мають назву *P*-

заборонених коаліцій учасників БССРК із структурою специфікації Г. Як правило, вважається, що $\Im_P$ є монотонно незростаючим класом множин, тобто задовольняє умові $(C \in \Im_P, C' \subseteq C) \Rightarrow (C' \in \Im_P)$ [13]. У випадку, коли сукупність $\Im_P$ не залежить від конкретної привілейованої групи P (тобто є однією і тією ж для всіх $P \in \Re$) вона позначається символом $\Im$ та називається *сукупністю заборонених коаліцій* даної безумовно стійкої схеми розподілу ключів [10, 13, 73].

Неформальний зміст введених понять полягає в тому, що після розподілу секретної інформації з ЦРК кожен абонент $i \in V$, який належить до певної привілейованої групи $P \in \Re$, здатний обчислити груповий ключ k_P, що пов'язаний з P. З іншого боку, довільна заборонена коаліція $C \in \Im_P$ не має можливості отримати будь-яку інформацію про значення ключу k_P.

Далі для безумовно стійкої схеми розподілу ключів із структурою специфікації Г будемо використовувати назву Г-БССРК.

На цей час у багатьох наукових публікаціях значна увага приділяється дослідженню окремого класу БССРК, структура специфікації яких має вигляд $\Gamma = (\Re, \Im) = \{(P, C) \in \Re \times \Im : P \cap C = \varnothing\}$ [1, 9, 10, 13, 73 – 76]. Найбільш вивченими серед таких БССРК є схеми з *пороговими структурами специфікацій*, в яких сукупності $\Re$ та $\Im$ складаються з підмножин множини V, що мають значення потужностей не більше, ніж n та t відповідно. Зазначені схеми розподілу ключів називаються $(\le n, t)$-БССРК. Якщо сукупність $\Re$ складається зі всіх підмножин множини V потужності n, а сукупність $\Im$ містить усі коаліції потужності не більше t, то у цьому випадку $(\Re, \Im)$-БССРК має назву (порогової) (n, t)-БССРК.

Схема розподілу ключів із структурою специфікації $\Gamma = (\Re, \Im)$ називається *t-стійкою* (t = 0, 1, …) [9, 77], якщо $\Im \supseteq \{C \in 2^V : |C| \le t\}$, тобто кожна множина C потужності не більше t є P-забороненою коаліцією для всіх $P \in \Re$ таких, що $P \cap C = \varnothing$.

Сформулюємо математичні визначення трьох зазначених вище класів безумовно стійких схем розподілу ключів. Спочатку приведемо ряд додаткових понять та позначень.

Для кожного $i \in V$ позначимо символом U_i множину всіх секретних значень u_i, що отримує з ЦРК абонент i, а символом M_i – множину всіх можливих відкритих повідомлень m_i, що надходять до абонента i мережею зв'язку на етапі обчислення групового ключу. Нехай K_P позначає множину можливих значень групового ключу k_P, який відповідає довільній привілейованій групі $P = \{i_1, \ldots, i_r\} \in \Re$, $U_P = U_{i_1} \times \ldots \times U_{i_r}$.

Згідно загальновизнаному припущенню [1, 10, 13], передбачається, що на множині U_V задано деякий розподіл ймовірностей, згідно з яким центр розподілу ключів обирає секретну інформацію $u \in U_V$ для передачі значення u_i кожному учаснику $i \in V$. Аналогічно вважається, що для кожного $P \in \Re$ задані розподіли ймовірностей на множинах $M_P = M_{i_1} \times \ldots \times M_{i_r}$ та K_P. У подальшому

викладенні будемо використовувати ті ж самі позначення для скінченних множин (U_i, M_i, K_P та інших) і випадкових величин, що розподілені на цих множинах. Для будь-яких випадкових величин *X* та *Y* позначатимемо $H(X)$ та $H(X \mid Y)$ відповідно безумовну та умовну ентропію випадкової величини *X* (за умовою *Y*) [78].

Математичні моделі трьох класів безумовно стійких схем розподілу ключів визначаються наступним чином.

Схемою попереднього розподілу ключів [47, 1, 10, 13] називається така БССРК, на першому етапі якої відбувається формування та передача захищеним каналом зв'язку кожному абоненту $i \in V$ секретного значення u_i, за допомогою якого на другому етапі кожний абонент, що належить довільній привілейованій групі $P \in \Re$, здатний обчислити груповий ключ k_P. При цьому повинні виконуватись наступні умови:

(1) для кожних $P \in \Re$, $i \in P$ має місце рівність $H(K_P|U_i) = 0$;

(2) для кожних $P \in \Re$, $C \in \Im_P$ справедлива рівність $H(K_P|U_C) = H(K_P)$.

Схема узгодження ключів [1] визначається як така БССРК, перший етап якої аналогічний відповідному етапу СПРК, а другий етап полягає в обміні відкритою інформацією між учасниками певних привілейованих груп, в результаті якого кожний учасник $i \in V$ отримує відкрите повідомлення m_i. При цьому виконуються такі умови:

(1) для кожних $P \in \Re$, $i \in P$ має місце рівність $H(K_P|U_i, M_i) = 0$;

(2) для кожних $P \in \Re$, $C \in \Im_P$ справедлива рівність

$$H(K_P|U_C, M_1, .., M_v) = H(K_P). \quad (1)$$

Відмітимо, що, згідно відомої властивості ентропії [78], рівність (1) є формальним виразом умови, за якою учасники забороненої коаліції $C \in \Im_P$ не отримують будь-якої інформації про груповий ключ k_P, виходячи з власних секретних повідомлень u_i, $i \in C$ та всій відкритої інформації, що передається мережею зв'язку на другому етапі СУК.

Нарешті, *схемою багатоадресного розподілу ключів* [1, 9, 10, 13] є така БССРК, перший етап якої співпадає з першим етапом у визначенні СПРК, а другий етап полягає в передачі широкомовним каналом зв'язку всім абонентам 1, 2, …, *v* певного повідомлення m_P, яке пов'язане із заздалегідь визначеною привілейованою групою $P \in \Re$. При цьому повинні виконуватись такі умови [1, 10, 13]:

(1) груповий ключ k_P, що відповідає групі *P*, не залежить від секретного повідомлення u_V, яке передається абонентам з ЦРК на першому етапі, тобто $H(K_P|U_V) = H(K_P)$;

(2) кожний абонент $i \in P$ є здатним обчислити ключ k_P, виходячи з власної секретної інформації u_i, що отримана ним з ЦРК, та повідомлення m_P: $H(K_P|U_i, M_P) = 0$;

(3) учасники будь-якої забороненої коаліції $C \in \Im_P$ не можуть отримати жодної інформації про ключ k_P, тобто $H(K_P|U_C, M_P) = H(K_P)$.

Слід зауважити, що у приведених вище математичних визначеннях БССРК не розкривається конкретний зміст алгоритмічних процедур, за якими здійснюється формування повідомлень u_V, m_i $(i \in V)$, m_P та, відповідно, обчислення групового ключу k_P привілейованою групою учасників P. Такі процедури визначаються окремо при заданні конкретних схем розподілу ключів, аналізу властивостей яких присвячені наступні пункти цього розділу.

Для кількісної оцінки ефективності та проведення порівняльного аналізу різноманітних видів БССРК використовується ряд показників ефективності схем багатоадресного розподілу ключів, що визначають кількість секретної інформації, яка передається як кожному окремому абоненту, так і в цілому всім учасникам БССРК [10, 13]. Далі, не обмежуючи загальності, вважатимемо, що всі можливі значення групового ключу k_P у визначених вище класах БССРК належать певній скінченній множині K, яка не залежить від конкретної групи $P \in \Re$.

Першим показником ефективності будь-якої БССРК є її *інформаційна швидкість* ρ, що визначається як відношення довжини групового ключу k_P до максимальної довжини секретних повідомлень, які передаються абонентам з ЦРК, тобто $\rho = \dfrac{\log|K|}{\max_{i \in V} H(U_i)}$ [10]. Неформально кажучи, зазначена величина обернено пропорційна відношенню максимальної кількості секретної інформації, що необхідна довільному учаснику $i \in V$ для обчислення ключу k_P, до кількості інформації, яка міститься у цьому ключі.

Другим показником ефективності безумовно стійкої схеми розподілу ключів є її *повна інформаційна швидкість* ρ_T, яка визначається як відношення довжини групового ключу до кількості всієї секретної інформації, що передається абонентам із центру розподілу ключів. Отже, повна інформаційна швидкість схеми попереднього розподілу ключів визначається за формулою $\rho_T = \dfrac{\log|K|}{H(U_V)}$, а повна інформаційна швидкість схеми багатоадресного розподілу ключів – за формулою $\rho_T = \dfrac{\log|K|}{\max_{P \in \Re} H(U_V, M_P)}$ [10]. За своєю сутністю параметр ρ_T обернено пропорційний загальної кількості секретної інформації, що генерується в ЦРК на обох етапах даної БССРК.

Нарешті, для характеристики ефективності схем багатоадресного розподілу ключів використовується ще один показник – *багатоадресна інформаційна швидкість* ρ_M, що визначається як відношення довжини групового ключу k_P до максимальної довжини повідомлення m_P, яке передається з ЦРК широкомовним каналом зв'язку всім абонентам мережі [10, 13]: $\rho_M = \dfrac{\log|K|}{\max_{P \in \Re} H(M_P)}$. Даний параметр обернено пропорційний до

максимальної кількості відкритої інформації, яку необхідно передати учасникам будь-якої привілейованої групи для надання їм можливості однозначно відновити відповідний груповий ключ.

Зрозуміло, що на практиці найбільш ефективною за будь-яким із визначених вище показників вважається така БССРК, для якої цей показник досягає максимального можливого значення. Слід відмітити, що введені показники близько пов'язані між собою, внаслідок чого збільшення значення одного з них (наприклад, інформаційної швидкості СБРК), як правило, призводить до зменшення значення іншого (багатоадресної швидкості даної СБРК) та навпаки [10, 13].

Поряд із розглянутими вище, для характеристики ефективності окремих типів схем багатоадресного розподілу ключів використовується ряд інших показників, які або еквівалентні вищезазначеним, або точніше відображають відповідні властивості конкретних СБРК [9, 12, 77]. Визначення цих показників приведені в другої частині даної статті при аналізі відповідних схем багатоадресного розподілу ключів.

3. Аналіз методів побудови та ефективності безумовно стійких схем попереднього розподілу й узгодження ключів

За результатами сучасних наукових робіт в галузі побудови та аналізу властивостей безумовно стійких схем розподілу ключів [1, 10, 11, 13, 73, 75, 76, 79] можливо виділити три фундаментальні задачі, прогрес у вирішенні яких фактично визначає сучасний стан та напрямки подальшого розвитку цієї галузі криптографії.

1. Задача побудови верхніх границь параметрів, що характеризують ефективність безумовно стійких СПРК, СУК та СБРК. Такі границі дозволяють виявити та оцінити потенційні можливості перспективних безумовно стійких схем розподілу ключів [1, 11, 12, 73, 80].

2. Задача обґрунтування досяжності зазначених границь для БССРК з найбільш важливими, з практичної точки зору, структурами специфікацій та синтезу оптимальних БССРК (тобто таких, значення показників ефективності яких досягають отриманих границь) [1, 9, 47, 74, 80, 81].

3. Задача розробки методів побудови безумовно стійких схем розподілу ключів, які мають не завжди оптимальні, але практично прийнятні параметри ефективності [3, 9, 10, 12, 13, 73, 76, 77, 79, 82]. Головними напрямами досліджень, що спрямовані на вирішення даної задачі, є пошук "компромісу" між основними показниками ефективності БССРК (наприклад, інформаційною швидкістю та багатоадресною інформаційною швидкістю СБРК) та підвищення інформаційних швидкостей БССРК за рахунок деякого послаблення вимог до їхніх структур специфікацій [3, 10, 13, 82].

Нижче викладені результати аналізу методів побудови та ефективності найбільш відомих схем попереднього розподілу й узгодження ключів у спеціальних телекомунікаційних системах. Аналізу методів побудови більш перспективного класу схем багатоадресного розподілу ключів присвячена наступна чатина даного огляду.

Історично першими БССРК є схеми попереднього розподілу ключів [47, 74]. Найпростішим та широко відомим прикладом СПРК є так звана *тривіальна*

схема попереднього розподілу ключів, яка визначається для порогової структури специфікації з параметрами (n,t). В цій схемі кожний учасник довільної привілейованої групи P, де $|P|=n$, отримує з ЦРК рівно одне секретне повідомлення (для кожного P), яке співпадає з груповим ключем k_P. Тривіальна СПРК має інформаційну швидкість $\rho=\binom{t-1}{n-1}^{-1}$ та повну інформаційну швидкість $\rho_T=\binom{t}{n}^{-1}$ [10]. Очевидним недоліком такої СПРК є те, що число секретних повідомлень, які повинен генерувати ЦРК, у загальному випадку експоненційно зростає зі збільшенням кількості абонентів мережі зв'яку. Також експоненційно зростає число ключів, що зберігає кожен абонент [1].

З метою економії числа ключів, що має генерувати ЦРК та зберігати абоненти мережі зв'язку, в [47] запропонована конструкція безумовно стійкої $(2,t)$-СПРК, $t\geq 1$, що основується на симетричних поліномах від двох змінних над скінченним полем. В [47, 10] показано, що дана СПРК (так звана *схема Блома*) має інформаційну швидкість та повну інформаційну швидкість, які дорівнюють відповідно

$$\rho=\frac{1}{t+1},\ \rho_T=\binom{t+2}{2}^{-1}. \qquad (2)$$

Пізніше різноманітні конструкції СПРК для порогових структур специфікацій пропонувались в [9, 74, 81, 83] та інших роботах. Так, в [74] описана безумовно стійка схема попереднього розподілу ключів, яка узагальнює СПРК із [47], а саме, реалізує структуру специфікації з параметрами (n,t), де $t\geq 1$, $n\geq 2$, $t+n\leq v$. Така СПРК (с*хема* "*Бландо та інших*") будується на основі симетричних поліномів від n змінних, степені не більше t за кожною змінною, над полем із $q\geq v$ елементів та дозволяє довільній групі P з n учасників обчислювати спільний груповий ключ таким чином, що будь-яка заборонена коаліція потужністю t не отримує жодної інформації про цей ключ. В [74] показано, що зазначена СПРК має інформаційну швидкість $\rho=\binom{n+t-1}{n-1}^{-1}$, повну інформаційну швидкість $\rho_T=\binom{n+t}{t}^{-1}$ та є оптимальною за критерієм максимуму інформаційної швидкості серед усіх (n,t)-СПРК. Пізніше узагальнення твердження про оптимальність схеми "Бландо та інших" отримане в статті [1].

Інша проста конструкція оптимальної $(\leq v,t)$-СПРК запропонована А. Фиатом і М. Наором [9] та узагальнена в [81]. Схема попереднього розподілу ключів з [81] має структуру специфікації $(2^V,\Im)$, де $\Im$ – довільний клас підмножин множини V. Вона складається з двох алгоритмів: етапу розподілу секретних повідомлень та етапу обчислення ключа.

На першому етапі ЦРК для кожної забороненої коаліції $C \in \Im$ обирає випадкове та рівноймовірне значення $s_C \in \overline{0, q-1}$, яке передається захищеним каналом зв'язку кожному абоненту $i \in V \setminus C$. На другому етапі довільна привілейована група $P \in 2^V$ має можливість обчислити груповий ключ k_P, який дорівнює сумі по модулю q значень s_C за всіма $C \in \Im$, що не перетинаються з P.

В [10] показано, що *схема Фіата–Наора* [9] має інформаційну швидкість ρ та повну інформаційну швидкістю ρ_T, що визначаються за формулами

$$\rho = \left(\sum_{j=0}^{t} \binom{v-1}{j} \right)^{-1}, \ \rho_T = \left(\sum_{j=0}^{t} \binom{v}{j} \right)^{-1}. \qquad (3)$$

Як власно схема Фіата–Наора, так і її узагальнення [81] є оптимальними (у заданих класах) СПРК одночасно за критерієм максимуму інформаційної швидкості та, відповідно, повної інформаційної швидкості [1, 10].

Аналізуючи приведені вище аналітичні вирази параметрів, що характеризують ефективність відомих оптимальних СПРК [1, 9, 10, 47, 74, 81], неважко впевнитись в тому, що значення цих параметрів швидко спадають зі збільшенням числа t, яке визначає максимальний розмір забороненої коаліції в СПРК. Отже, безпосереднє практичне використання зазначених схем розподілу ключів у телекомунікаційних системах з великою кількістю абонентів стає дуже проблематичним за жорсткими вимогами до потужностей заборонених коаліцій.

В якості приклада, розглянемо $(2, v-2)$-схему Блома, за якою кожна пара учасників СПРК може обчислити спільний ключ із безумовною стійкістю відносно коаліції решти учасників. Згідно формулам (2), реалізація такої СПРК вимагає від ЦРК згенерувати $(\rho_T)^{-1} = \dfrac{v(v-1)}{2}$ секретних повідомлень для передачі абонентам мережі зв'язку. При цьому кожен абонент має зберігати $\rho^{-1} = v-1$ повідомлень, і за фактом оптимальності схеми Блома, останнє число не може бути зменшено. Зрозуміло, що при великих значеннях v будь-яка СПРК із зазначеною структурою специфікації є малопрактичною (це так звана "*проблема* v^2", що полягає у розподілі секретних ключів між кожною парою v учасників) [22, 74, 84].

Спроби подолання відмічених принципових труднощів, що пов'язані з практичним використанням запропонованих раніше схем попереднього розподілу ключів [9, 47, 74], привели до розвитку загальних методів побудови СПРК за менш жорсткими вимогами відносно їхніх структур специфікацій та пошуку "компромісних" співвідношень між характеристиками ефективності СПРК. На сьогоднішній день відомо ряд загальних методів синтезу схем попереднього розподілу ключів (див. рис. 1) [10, 75, 79, 83, 85 – 89]. Більшість з них дозволяє отримувати СПРК, що мають лише порогові структури специфікацій, та (зрозуміло) не оптимальні значення показників ефективності ρ або ρ_T. Іншим певним недоліком СПРК, які будуються з використанням цих методів, є неможливість реалізовувати розподіл ключів за такими алгоритмами,

що дозволяють ЦРК заздалегідь формувати значення ключів певних привілейованих груп учасників. А саме, у більшості конструкцій сучасних СПРК спільний груповий ключ k_P визначається лише на останньому етапі процедури його обчислення учасниками даної групи P, що, взагалі кажучи, не дозволяє надавати цьому ключу (за умовами функціонування СПРК) заздалегідь визначених значень [85]. Відмітимо, що останнім часом з використанням апарату лінійної алгебри в [85, 79] запропоновані загальні методи побудови СПРК, які позбавлені цього недоліку. Проте, при використанні відмічених методів з'являється інша проблема, що пов'язана з труднощами синтезу таких СПРК для заздалегідь визначених структур специфікацій.

Іншим можливим підходом до підвищення ефективності сучасних схем попереднього розподілу ключів є застосування так званих *інтерактивних БССРК*, за якими передбачається обмін відкритою інформацією між абонентами, що мають обчислити спільний секретний ключ [73, 74, 90 – 92]. Такими схемами розподілу є саме безумовно стійкі схеми узгодження ключів, перша з яких запропонована в [74]. Як відзначено вище, СУК дозволяє абонентам встановлювати відповідні групові ключі шляхом їхньої взаємодії та використання власної секретної інформації, що отримана ними на першому етапі з ЦРК [1].

За певними умовами, які пов'язані з відмовою від жорстких вимог до розмірів заборонених коаліцій, схеми узгодження ключів дозволяють зменшити кількість секретної інформації, яку мають зберігати абоненти мережі зв'язку [73, 74]. Однак, як свідчать результати робіт [1, 90, 91], в загальному випадку використання СУК не дозволяє підвищити ефективність безумовно стійких схем розподілу ключів у порівнянні зі СПРК.

Уникнути відмічених недоліків та зберегти найкращі властивості БССРК, що сформульовані вище, дозволяють схеми багатоадресного розподілу ключів.

Список литературы: **1.** *Cimato S., D'Arco P., Cresti A.* A unified model for unconditional secure key distribution // http://www.dia.unisa.it/paodar.dir. **2.** *Canetti R., Garay J., Itkis G., Micciancio D., Naor M., Pinkas B.* Issue in multicast security: a taxonomy and efficient constructions // INFOCOM'99. – 1999. – P. 708 – 716. **3.** *Canetti R., Malkin T., Nissim K.* Effcient communication-storage tradeoffs for multicast encryption // Advances in Cryptology – EUROCRYPT'99, Lecture Notes in Computer Science. – 1999. – P. 459 – 474. **4.** *Poovendran R., Baras J.S.* An information theoretic analysis of rooted-tree based secure multicast key distribution schemes // Advances in Cryptology – CRYPTO'99. – 1999. – P. 624 – 638. **5.** *Safavi-Naini R., Wang H.* New constructions for multicast re-keying schemes using perfect hash families // 7th ACM Conf. on Computer and Communication Security, ACM Press. – 2000. – P. 228 – 234. **6.** *Wallner D.M., Harder E.J., Agee R.C.* Key management for multicast: issues and architectures // ftp://ftp.ieft.org/internet-drafts/draft-wallner-key-arch-01.txt. **7.** *Mittra S.* Iolus: a framework for scalable secure multicasting // ACM SIGCOMM'97, 1997. **8.** *Wong C.K, Gauda M., Lam S.S.* Secure group communications using key graphs // ACM SIGCOMM'98, 1998. **9.** *Fiat A., Naor M.* Broadcast encryption // Advances in Cryptology – EUROCRYPT'93, Lecture Notes in Computer Science. – 1994. – P. 480 – 491. **10.** *Stinson D.R.* On some methods for unconditionally secure key distribution and broadcast encryption // Designs, Codes and Cryptography. – 1997. – Vol. 12. – P. 215 – 243. **11.** *Blundo C., D'Arco P., Daza V., Padro C.* Bounds and constructions for unconditionally secure distributed key distribution schemes for general access structures // ISC'01, Lecture Notes in Computer Science, Springer-Verlag. – 2001. – P. 1 – 17. **12.** *Luby M., Staddon J.*

Combinatorial bounds for broadcast encryption // Advances in Cryptology – EUROCRYPT'98, Lecture Notes in Computer Science. – 1998. – P. 512 – 527. **13.** *Padro C., Gracio I., Martin S., Morillo P.* Linear broadcast encryption schemes // Discrete Appl. Math. – 2003. – Vol. 128. – P. 223 – 238. **14.** *Attrapadung N., Kobara K., Imai H.* Sequential key derivation patterns for broadcast encryption and key predistribution schemes // ASIACRYPT'03, Lecture Notes in Computer Science. – 2003. – P. 374 – 391. **15.** *Naor D., Naor M., Lotspiech J.* Revocation and tracing schemes for stateless receivers // Advances in Cryptology – CRYPTO'01, Lecture Notes in Computer Science. – 2001. – P. 41 – 62. **16.** *Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.* Основы криптографии. – М.: Гелиос АРВ, 2001. – 480 с. **17.** *Погорелов БА., Черемушкин А.В., Чечета С.И.* Об определении основных криптографических понятий // Математика и безопасность информационных технологий. Материалы конференции в МГУ 23 – 24 октября 2003 г. – М.: МЦНМО, 2003. – С. 75 – 85. **18.** *Фомичев В.М.* Дискретная математика и криптология. Курс лекций. – М.: Диалог-МИФИ, 2003. – 400 с. **19.** *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002. – 816 с. **20.** *Diffie W., Hellman M.E.* New directions in cryptography // IEEE Trans. on Inform. Theory. – 1976. – Vol. 22, № 6. – P. 644 – 654. **21.** *Maurer U.* Information-theoretic cryptography // Advances in Cryptology – CRYPTO'99, Lecture Notes in Computer Science. – 1999. – P. 47 – 64. **22.** *Cachin C.* Entropy measures and unconditional security in cryptography: Diss. … doc. Tech. Sciences. – Zurich, 1997. – 155 p. **23.** *Wolf S.* Information-theoretically and unconditionally secure key agreement in cryptography: Ph. D. Thesis № 13138. – ETH Zurich, 1999. **24.** *Dziembowski S., Maurer U.* Optimal randomized efficiency in the bounded-storage model // J. of Cryptology. – 2004. – Vol. 17, № 1. – P. 5 – 26. **25.** *Bennett C.H., Brassard G., Ekert A.K.* Quantum cryptography // Scientific American. – 1992. – P. 50 – 57. **26.** *Brassard G.* Recent developments in quantum cryptography // PRAGOCRYPT'96. – Prague. – 1996. **27.** *Needham R.M., Shroeder M.D.* Using encryption for authentication in large networks of computers // Communications of ACM. – 1978. – Vol. 21, № 12. – P. 993 – 999. **28.** *Чмора А.Л.* Современная прикладная криптография. – М.: Гелиос АРВ, 2002. – 256 с. **29.** *Bennett C.H., Brassard G.* Quantum cryptography and its application to provably secure key expansion, public-key distribution, and coin-tossing // IEEE International Symposium on Inform. Theory. – 1983. – P. 91. **30.** *Bennett C.H., Brassard G.* Quantum cryptography: Public-key distribution and coin tossing // Proc. of IEEE International Conf. on Computers, Systems and Signal Processing. – Bangalore (India), 1984. – P. 175 – 179. **31.** *Bennett C.H., Brassard G.* Quantum public key distribution reinvented // Sigact News. – 1987. – Vol. 18, № 4. – P. 51 – 53. **32.** *Bennett C.H., Bessette F., Brassard G., Salvail L., Smolin J.* Experimental quantum cryptography // J. of Cryptology. – 1992. – Vol. 5, № 1. – P. 3 – 28. **33.** *Wyner A.D.* The wire-tap channel // Bell Syst. Techn. J. – 1975. – Vol. 54, № 8. – P. 1335 – 1368. **34.** *Csiszar I., Korner J.* Broadcast channels with confidential messages // IEEE Trans. on Inform. Theory. – 1978. – Vol. 24, № 3. – P. 339 – 348. **35.** *Горицкий В.М.* Вероятностная криптография в системах защиты информации: кодовая защита // Электроника и связь. – 1998. – Вып. 5. – С. 140 – 145. **36.** *Maurer U.* Secret key agreement by public discussion from common information // IEEE Trans. on Inform. Theory. – 1993. – Vol. 39. – № 3. – P. 733 – 742. **37.** *Ahlswede R., Csiszar I.* Common randomness in information theory and cryptography. – Patr. 1: Secret scharing // IEEE Trans. on Inform. Theory. – 1993. – Vol. 39, № 4. – P. 1121 – 1132. **38.** *Bennett C.M., Brassard G., Crepeau C., Maurer U.* Generalized privacy amplification // IEEE Trans. on Inform. Theory. – 1995. – Vol. 41, № 26. – P. 1915 – 1923. **39.** *Maurer U., Wolf S.* Towards characterizing when information-theoretic key agreement is possible // ASIACRYPT'96, Lecture Notes in Computer Science. – 1996. – P. 196 – 209. **40.** *Чисар И.* Почти независимость случайных величин и пропускная способность криптостойкого канала // Проблемы передачи информации. – 1996. – Т. 32, Вып. 1. – С. 48 – 57. **41.** *Maurer U.* Information-theoretically secure secret-key agreement by not authenticated public discussion // Advances in Cryptology. – EUROCRYPT'97, Lecture Notes in Computer Science. – 1997. – P. 209 – 225. **42.** *Maurer U., Wolf S.* Information-theoretic key agreement: from weak to strong secrecy for free // Advances in Cryptology – EUROCRYPT'00, Lecture Notes in Computer Science. – 2000. – P. 351 – 368. **43.** *Maurer U., Wolf S.* Secret-key agreement over unauthenticated public channels. – Part I – III // IEEE Trans. on Inform. Theory. – 2003. – Vol. 49, № 4. – P. 822 – 851. **44.** *Maurer U.*

A provable-secure strongly randomized cipher // Advances in Cryptology – EUROCRYPT'90, Lecture Notes in Computer Science. – 1990. – P. 361 – 373. **45.** *Cachin C., Maurer U.* Unconditional security against memory-bounded adversaries // Advances in cryptology – CRYPTO'97, Lecture Notes in Computer Science. – 1997. – P. 292 – 306. **46.** *Koenig R., Maurer U., Renner R.* Privacy amplification secure against an adversary with selectable knowlege // IEEE International Symp. on Inform. Theory. – 2004. – P. 231. **47.** *Blom R.* An optimal class of symmetric key generation systems // Advances in Cryptology – EUROCRYPT'84, Lecture Notes in Computer Science. – 1994. – P. 335 – 338. **48.** *Anzai J., Matsuzaki N., Matsumoto T.* A quick group key distribution scheme with entity revocation // ASIACRYPT'99, Lecture Notes in Computer Science. – 1999.– P. 333 – 347. **49.** *Asano T.* A revocation Scheme with minimal storage at receivers. // ASIACRYPT'02, Lecture Notes in Computer Science. – 2002. – P. 433 – 450. **50.** *Dodis Y., Fazio N.* Public key broadcast encryption for stateless receivers // ACM Workshop on digital rights management. – 2002. **51.** *Dodis Y., Fazio N., Kiayias A., Yung M.* Fully scalable public-key traitor tracing // PODC'03. – 2003. **52.** *Naor M., Pincas B.* Efficient trace and revoke schemes // FC'00, Lecture Notes in Computer Science. – 2000. – P. 1 – 20. **53.** *Halevy D., Shamir A.* The LSD broadcast encryption scheme // Advances in Cryptology – CRYPTO'02, Lecture Notes in Computer Science. – 2002. – P. 47 – 60. **54.** *Вербіцький О.В.* Вступ до криптології. – Львів: ВНТЛ, 1998. – 247с. **55.** *Chor B., Fiat A., Naor M., Pinkas B.* Traitor tracing // IEEE Trans. on Inform. Theory. – 2000. – Vol. 46, №. 3. – P. 893 – 910. **56.** *Pfitzmann B.* Trials of traced traitors // Information Hiding, Lecture Notes in Computer Science. – 1996. – Vol. 1174. – P. 49 – 64. **57.** *Dwork C., Lotspiech J., Naor M.* Digital signets: self-enforcing protection of digital information // 28-th Symposium on the Theory of Computation. – 1996. – P. 489 – 498. **58.** *Boneh D. Franklin M.* An efficient public key traitor scheme // Advances in Cryptology – CRYPTO'99, Lecture Notes in Computer Science. – 1999. – P. 338 – 353. **59.** *Stinson D.R., Wei R.* Combinatorial properties and constructions of traceability schemes and frameproof codes // SIAM J. on Discrete Mathematics. – 1998. – Vol. 11. – P. 41 – 53. **60.** *Berkman O., Parnas M., Sgall J.* Efficient dynamic traitor tracing // SODA'00. – 2000. – P. 586 – 595. **61.** *Garay J., Staddon J., Wool A.* Long-lived broadcast encryption // Advances in Cryptology – CRYPTO'00, Lecture Notes in Computer Science. – 2000.– P. 333 – 352. **62.** *Fiat A., Tessa T.* Dynamic traitor tracing // J. of Cryptology. – 2001. – Vol. 14. – P. 211 – 223. **63.** *Safavi-Naini R., Wang Y.* Sequential traitor tracing // Lecture Notes in Computer Science. – 2000. – Vol. 1880. – P. 316 – 332. **64.** *Staddon J.N., Stinson D.R., Wei R.* Combinatorial properties of frameproof and traceability codes // IEEE Trans. on Inform. Theory. – 2001. – Vol. 47. – P. 1042 – 1049. **65.** *Kiayias A., Yung M.* Self protecting pirates and black-box traitor tracing // Advances in Cryptology – CRYPTO'01, Lecture Notes in Computer Science. – 2001. – P. 63 – 79. **66.** *Kiayias A., Yung M.* Traitor tracing with constant transmission rate // Advances in Cryptology – EUROCRYPT'02, Lecture Notes in Computer Science. – 2002. – P. 450 – 465. **67.** *Bennett C.H., Brassard G., Robert J. – M.* Privacy amplification by public discussion // SIAM J. on Comput. – 1988. – Vol. 17, № 2. – P. 210 – 229. **68.** *Kumar R., Rajagopalan S., Sahai A.* Coding constructions for blacklisting problems without computational assumptions // Advances in Cryptology – CRYPTO'99, Lecture Notes in Computer Science. – 1999. – P. 609 – 623. **69.** *Kurnio H., Safani-Naini R., Wang H.* A Group key distribution scheme with decentralised user join // SCN'02, Lecture Notes in Computer Science. – 2002. **70.** *Gafni E., Staddon J., Yin Y.L.* Efficient methods for integrating traceability and broadcast encryption // Advances in Cryptology – CRYPTO'99, Lecture Notes in Computer Science. – 1999. – P. 372 – 387. **71.** *Stinson D.R., Wei R.* Key preassigned traceability schemes for broadcast encryption // SAC'98, Lecture Notes in Computer Science. – 1999. – Vol. 1556. – P. 144 – 156. **72.** *Stinson D.R., Wei R.* An application of ramp schemes to broadcast encryption // Information Processing Letters. – 1999. – Vol. 69. – P. 131 – 135. **73.** *Blundo C., Frota Mattos L.A., Stinson D.R.* Trade-offs between communication and storage in unconditionally secure schemes for broadcast encryption and interactive key distribution // Advances in Cryptology – CRYPTO'96, Lecture Notes in Computer Science. – 1996. – P. 387 – 400. **74.** *Blundo C., de Santis A., Herzberg A., Kutten S., Vaccaro U., Yung M.* Perfectly-secure key distribution for dynamic conferences // Advances in cryptology – CRYPTO'92, Lecture Notes in Computer Science. – 1993. – P. 471 – 486. **75.** *Stinson D.R., van Trung T.* Some new results on key distribution patterns and broadcast encryption // Designs, Codes and Cryptography. – 1998. – Vol.

15. – P. 261 – 279. **76.** *D'Arco P., Stinson R.D.* On unconditionally secure robust distributed key distribution centers // ASIACRYPT'02, Lecture Notes in Computer Science. – 2002. – P. 346 – 363. **77.** *Korjik V., Ivkov M., Merinovich Y., Bang A., van Tilborg H.* A broadcast key distribution scheme based on block designs // Lecture Notes in Computer Science. – 1995. – № 1025. – P. 12 – 21. **78.** *Шеннон К.* Теория связи в секретных системах / Работы по теории информациии кибернетике. – М.: ИЛ., 1963. – С. 333 – 402. **79.** *Padro C., Gracia I., Martin S., Morillo P.* Linear key predistribution schemes // Designs, Codes and Cryptography. – 2002. – Vol. 25. – P. 281 – 298. **80.** *Beimel A.* Secure schemes for secret sharing and key distribution: Diss. … doctor of sciences. – Haifa, 1996. – 115 p. **81.** *Blundo C., Cresti A.* Space requirements for broadcast encryption // Advances in Cryptology – EUROCRYPT'94, Lecture Notes in Computer Science. – 1994. – P. 287 – 298. **82.** *Gracia I., Martin S., Padro C.* Improving the trade-off betveen storage and communication in broadcast encryption schemes // http://www.iacr.org/2001/088. **83.** *Matsumoto T., Imai H.* On the key predistribution system: a practical solution to the key distribution problem // Advances in Cryptology – CRYPTO'87, Lecture Notes in Computer Science. – 1987. – P. 185 – 193. **84.** *Gong L., Wheeler D.J.* A Matrix key-distribution scheme // J. of Cryptology. – 1990. – Vol. 2. – P. 51 – 59. **85.** *Saez G.* Generation of key predistribution schemes using secret sharing schemes // WCC'01. – France. – 2001. – P. 435 – 444. **86.** *Blundo C., de Santis A., Vaccaro U.* Randomness in distribution protocols // Advanced in Cryptology – CRYPTO'92, Lecture Notes in Computer Science. – 1993. – P. 471 – 486. **87.** *O'Keefe C.M.* Applications to information security // Australasian J. combinatorics. – 1993. – № 7. – P. 195 – 212. **88.** *Quinn K.A.S.* Some constructions for key distribution patterns // Designs, Codes and Cryptography. – 1994, № 4. – P. 177 – 191. **89.** *Kurosawa K., Yoshida T., Desmedt Y., Burmester M.* Some bounds and a construction for secure broadcast encryption // ASIACRYPT'98, Lecture Notes in Computer Science. – 1998. – P. 420 – 433. **90.** *Beimel A., Chor B.* Interaction in key distribution schemes // Advances in Cryptology – CRYPTO'93, Lecture Notes in Computer Science. – 1993. – P. 444 – 455. **91.** *Beimel A., Chor B.* Communication in key distribution schemes // IEEE Trans. on Inform. Theory. – 1996. – Vol. 42. – P. 19 – 28. **92.** *Blundo C., D'Arco P., Giorgio Gaggia A.* A τ-restricted key agreement scheme // The Comp. J. – 1999. – Vol. 42, № 1. – P. 51 – 61.